FEDERAL DEFENDER OFFICE
DISTRICT OF MASSACHUSETTS
408 ATLANTIC AVENUE, 3RD FLOOR
BOSTON, MASSACHUSETTS 02110

TELEPHONE: 617-223-8061
FAX: 617-223-8080

December 8, 2008

Hon. Ricardo H. Hinojosa, Chair
United States Sentencing Commission
One Columbus Circle, N.E.
Washington, DC 20002-8002

Re: Public comment on Commission action in response to Pub. L. 110-326, § 209 (a directive relating to identity theft and computer crimes).

Dear Judge Hinojosa:

I want to thank you and your staff again for asking me to speak on behalf of the Federal Defenders at the Commission's briefing on November 20, 2008. I did not submit a written statement on that date, but would like to do so now with the comments set forth below. The directive in § 209 of Pub. L. 110-326 asks the Commission to study thirteen factors in the context of five statutes. These comments are not meant to address each factor in all its possible permutations. I do, however, seek to share with you some of our initial responses to the directive, in the hope that they will be useful to you at this stage of the amendment cycle. We look forward to working with the Commission and submitting further comment as the amendment process unfolds.

At the outset, I should note that we are struck by the fact that the Commission has already studied and responded to the substance of many of the factors enumerated in § 209, particularly with respect to offenses proscribed by 18 U.S.C. § 1030. Absent evidence that the guidelines in their present form do not adequately address concerns raised in the directive, we see little need for further action. Moreover, to the extent that any amendments to the guidelines would raise sentences in identity theft cases, we note that with the passage of the Identity Theft Penalty Enhancement Act in 2004, Congress provided for a two-year, minimum mandatory consecutive sentence to be imposed where identity theft is committed in relation to a broad range of federal felony offenses. *See* 18 U.S.C. § 1028A(a)(1) and (b). It is the position of the Federal Defenders that this statute punishes severely enough, and in many instances too severely, the crime of identity theft and the concomitant invasion of privacy which that offense entails.

We offer the following additional observations, which I have arranged to correspond generally to the factors as they appear and are numbered in the directive.

§ 209(b)(1) The level of sophistication and planning involved in such offense.

The Commission addressed this factor with respect to 18 U.S.C. § 1030 offenses in 2003. In section 225(b)(2) of the Homeland Security Act of 2002, Pub. L. 107-296, Congress directed the Commission to ensure that the guidelines and policy statements applicable to § 1030 offenses adequately account for the level of sophistication involved in the offense. *See* USSG, App. C, Amend. No. 654 (Nov. 1, 2003). After reviewing data on 116 cases, the Commission concluded that the special offense characteristic now at USSG § 2B1.1(b)(9)(C), which adds two levels "if the offense . . . involved sophisticated means," adequately accounts for increased culpability when the offense involves "especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense." USSG § 2B1.1 comment. (n.8(B)); *see* USSC, *Report to Congress: Increased Penalties for Cyber Security Offenses*, at 8 (May 2003) [*Cyber Crimes Report*]. At the time, the Commission's data "suggest[ed] that many 18 U.S.C. § 1030 offense are relatively unsophisticated."

At the hearing held on November 20th, the representative of the Department of Justice suggested that the Commission should now amend Application Note 8(B) to specify that the use of computer proxies constitutes "sophisticated means." As described by the Department, offenders are increasingly using proxies to commit computer crimes, making it harder to detect the offense and apprehend the offender.

We believe that the Commission should not add another enumerated example to Application Note 8(B). First, the term "sophisticated means" as defined in the first sentence of Application Note 8(B) is broad enough to encompass situations in which the use of a proxy constitutes sophisticated means.[1] The Department has not suggested that courts have been unable to account for the use of proxies, or have been forced to depart at substantial rates, because of the absence of an enumerated example. Without some evidence that the guidelines do not adequately account for the use of proxies, the Commission should not act.

Second, it is not at all clear that the use of proxies always involves especially complex or intricate conduct, or that it always makes the offense more difficult to detect. As technology advances, what once was sophisticated becomes commonplace. We would hazard to guess that a significant number of people today consider the use of a proxy to be a relatively basic technological function that is neither intricate nor complex. The Commission should avoid creating what would amount to a presumptive enhancement for the use of a proxy – applicable to every case governed by § 2B1.1 – unless the government can demonstrate that the technique used in a given case necessarily involved the special complexity and intricacy for which the enhancement was intended.

---

[1] The first sentence of Application Note 8(B) provides that "'sophisticated means' means especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense."

Third, adding proxies as an enumerated example runs counter to the Commission's goal of simplifying the guidelines. By the time the Commission has amended Application Note 8 to add proxies as an example, technology may well have advanced to yet another form of sophisticated concealment in computer crimes, rendering proxies obsolete and requiring yet another example to keep pace. Indeed, any example of "especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense" is subject to rapid obsolescence. Instead of continually adding or amending examples in response to cutting-edge technology, the Commission should leave it to the sentencing court to determine whether the use of the particular technology in the case before it constitutes sophisticated means.

§ 209(b)(2) Whether such offense was committed for purpose of commercial advantage or private financial benefit.

The Commission also addressed this factor with respect to 18 U.S.C. § 1030 offenses in 2003. At the time, the Commission did not amend the guidelines to increase sentences under § 2B1.1 based on this factor because "commercial advantage and private financial benefit are typical motivations in offenses sentenced under § 2B1.1, . . . and the structure of the guideline takes this into account." *Cyber Crimes Report* at 8-9. There is no indication that this conclusion is no longer sound with respect to offenses sentenced under § 2B1.1.

With respect to 18 U.S.C. § 2511 wiretapping offenses sentenced under § 2H3.1, we do not believe that the Commission should amend that guideline to provide for increased punishment if the offense was committed for the purpose of commercial gain or private financial benefit. First, § 2H3.1 already provides for a three-level enhancement if the purpose of the offense was to obtain direct or indirect commercial advantage or economic gain, bringing the base offense level to 12. *See* USSG § 2H1.3(b)(1)(B). Depending on a defendant's criminal history, the resulting sentence recommended by the guidelines is a term of imprisonment ranging from 10 to 37 months, *see* USSG ch. 5, pt. A (Sentencing Table).

Second, increasing the offense level to further account for commercial gain would reduce the utility of the upward departure provisions at Application Note 5 of § 2H3.1. Under the current structure of § 2H3.1, courts can account for commercial gain and still find room to depart upward as necessary in those cases in which the offense level does not adequately account for the seriousness of the invasion of privacy or value of protected information. If the offense level is automatically increased in all cases resulting in commercial gain, courts will have less room to account for the gradations in harms addressed by Application Note 5.

The Commission should only consider amending the guidelines if its review of data indicates a significant rate of upward departure in wiretap cases on the basis that § 2H3.1 does not adequately account for commercial or private gain. If the Commission does amend the guideline, it should take the opportunity to eliminate the flat three-level increase for any amount of commercial gain in order to ensure that a defendant whose financial gain is minimal is no longer considered the same as a

defendant whose financial gain is substantial. *See*, *e.g.*, § 2B5.3 (Criminal Infringement of Copyright or Trademark) (adding no levels if the infringement amount is $2,000 or less, and only one level if the infringement amount exceeds $2,000 but is less than $5,000).

§ 209(b)(3) The potential and actual loss resulting from the offense[.]

Congress has directed the Commission to consider whether the guidelines adequately account for "the value of information obtained from a protected computer, regardless of whether the owner was deprived of use of the information," and in the case of trade secrets or other proprietary information, "the cost the victim incurred developing or compiling the information." *See* Pub. L. No. 110-326, § 209(b)(3).

We have not found any evidence that courts are finding it difficult to calculate potential or actual loss as currently defined in § 2B1.1 in the circumstances described by the directive. Indeed, it appears that courts readily consider the development costs of proprietary information in calculating loss. In *United States v. Ameri*, 412 F.3d 893 (8th Cir. 2005), the defendant was convicted, *inter alia*, of theft of trade secrets in the form of computer software for which there was no verifiable "fair market value" and no "repair" of the software was involved. *Id.* at 895. The court held that the district court did not err in its calculation of loss, which included as a major component the cost of development. *Id.* at 900-01. And in *United States v. Four Pillars Enter. Co*., 253 Fed. Appx. 502 (6th Cir. 2007), the district court granted the government's request to consider the research and development cost of proprietary formulas obtained by the defendant, which the government then proved to be approximately $869,300. *Id.* at 512 (affirming the calculation of loss).

In addition, Application Note 3(C) states that in estimating loss, a court can consider "[t]he reduction that resulted from the offense in the value of equity securities or *other corporate assets*." (emphasis added.) This language should adequately cover dilution in the value of a corporation's proprietary information.

For any remaining case that might involve loss not specifically addressed in the guideline and Application Note 3, courts may consult Application Note 19, which allows for upward departure if "the offense caused or risked substantial non-monetary harm" or if "the offense created a risk of substantial loss beyond the loss determined for purposes of subsection (b)(1)." USSG § 2B1.1 comment. (n.19(A)(ii), (iv)) (2008).

Contrary to the suggestion by the Department, the result in *United States v. Levine*, 477 F.3d 596 (8th Cir. 2001), does not suggest that the guidelines need to be amended to account for the cost to the victim of developing proprietary information. The government in *Levine* did not ask the district court to consider the development costs incurred by Acxiom Corporation, the victim in the case, in calculating loss under § 2B1.1. Rather, the government requested the court to calculate loss based on the government expert's estimate of the fair market value of the information illegally obtained (an estimate of over $58 million). *See United States v. Levine*, No. 4:04CR00175 (E.D.

Ark.), Gov't Sentencing Mem. at 6-10. The defendant challenged that calculation, arguing that, based on the opinion of his own expert witnesses, the fair market value of the information obtained was less than $5,000. *See id.,* Def.'s Sentencing Mem. at 18. In the alternative, the defendant argued that the maximum reasonable loss calculation could be based on the value of the information as stipulated in a related case, also based on the fair market value, which placed the loss at $893,000. *See Levine*, 477 F.3d at 603. The court ultimately calculated the loss at $850,000, presumably based on the competing suggestions of fair market value. Although the court did depart upward, it did not do so to account for development costs or dilution in the value of the information. *See United States v. Levine*, No. 4:04CR00175 (E.D. Ark.), Sent. Tr. at 348-49.

In short, we believe that, absent evidence that courts are too often forced to rely on upward departures in order to account for the kinds of loss addressed by this directive, the Commission should not add unnecessary complexity to a guideline that is already quite complex.

§ 209(b)(4) Whether the defendant acted with intent to cause either physical or property harm in committing the offense.

The Commission also addressed this factor with respect to 18 U.S.C. § 1030 offenses in 2003. At the time, the Commission increased punishment by approximately 50% for damage to a protected computer under 18 U.S.C. § 1030(a)(5)(A)(i) to account for increased penalties "and the heightened level of intent involved in such violations." *See Cyber Crimes Report*, at 4, 9; USSG App. C, Amend. No. 654 (Nov. 1, 2003); USSG § 2B1.1(b)(15)(ii) (2008).

In addition to incrementally increasing punishment on the basis of the pecuniary damage caused, § 2B1.1 provides for a two-level enhancement if the offense involved "the conscious or reckless risk of death or serious bodily injury," USSG § 2B1.1(b)(13) (2008), and the commentary suggests an upward departure where the offense level substantially understates the seriousness of the offense "if the primary objective of the offense was an aggravating, non-monetary objective," or "[t]he offense caused or risked substantial non-monetary harm." *See* USSG § 2B1.1, comment. (n.19(A)(i) and (ii)). Death resulting from a § 1030 offense was specifically enumerated in 2003 as a basis for upward departure. *See* USSG § 2B1.1, comment. (n.19(A)(ii)).

Finally, § 2B1.1 contains a cross-reference if "the conduct set forth in the count of conviction establishes an offense specifically covered by another guideline in Chapter Two." *Id*. § 2B1.1 (c)(3)(C).

With the foregoing provisions, courts have sufficient guidance to account for a defendant's intent to cause physical or property damage.

§ 209(b)(5) The extent to which the offense violated the privacy rights of individuals.

§ 209(b)(8) Whether the offense involved a computer used by the United States Government, a State, or a local government in furtherance of national defense, national security, or the administration of justice.

§ 209(b)(11) Whether the defendant's intent to cause damage or intent to cause personal information should be disaggregated and considered separately from other factors set forth in § 2B1.1(b)[(15)].

In 2003, in response to Congress's directive, the Commission added a two-level enhancement in § 2B1.1 for 18 U.S.C. § 1030 offenses where the offense involved (1) "a computer system used to maintain or operate a critical infrastructure or used by or for a government entity in furtherance of the administration of justice, national defense, or national security," or (2) "an intent to obtain personal information." USSG, App. C., Amend. No. 654 (Nov. 1, 2003); USSG § 2B1.1(b)(15)(A)(i)(I-II) (2008).

As structured, this enhancement (which corresponded to an approximate 25% increase in sentences) will be superseded by greater enhancements under the same subsection if the offense also involved intentionally damaging a protected computer under 18 U.S.C. § 1030(a)(5)(A)(i) (resulting in a 50% increase in sentence) or if it caused substantial disruption of a critical infrastructure (roughly doubling the sentence). As the Commission explained to Congress, the graduated levels "ensure incremental punishment for increasingly serious conduct, and were chosen by the Commission in recognition of the fact that conduct supporting application of a more serious enhancement will frequently encompass behavior relevant to a lesser enhancement as well." *See Cyber Crimes Report*, at 4.

At the time, the Commission indicated that approximately 33% of the cases it studied would have received a two-level enhancement based on the defendant's intent to obtain personal information. Another very small number of defendants would have received a two-level increase because the offense involved a computer system used to maintain a critical infrastructure. Another 14.4% would have received the four-level adjustment for intentional damage to a protected computer. No case would have received the six-level enhancement for disrupting a critical infrastructure. *See id.*[2]

In keeping with the Commission's rationale for structuring these enhancements in a manner which provides for incremental punishment, we do not believe that the Commission should disaggregate the factors in subsection (b)(15)(A)(i) from each other or from the other factors. First, changing these factors to cumulative enhancements for 18 U.S.C. § 1030 offenses would risk

[2] It is not clear from the data how many offenses involved conduct covered by more than one enhancement, if any.

excessive punishment. Second, separate enhancements based on these factors that might apply to all offenses covered by § 2B1.1 would stray beyond the discrete statutory provisions addressed by Congress's directive here.

In addition, Application Note 19 already allows courts to increase sentences as necessary in those cases in which the guideline range understates the seriousness of the offense. For example, if aggregation under subsection (b)(15) results in a single upward enhancement that does not adequately account for the harm caused to privacy interests, the court can depart upward if the "offense caused or risked substantial non-monetary harm," such as a "substantial invasion of privacy interest." USSG § 2B1.1 comment. (n.19(A)(ii)) (2008). The court could also account for aggravated harms in the case of stolen information from a protected computer under 18 U.S.C. § 1030(e)(2) if the defendant sought the stolen information to further a broader criminal purpose. *Id.* § 2B1.1 comment. (n.19(A)(v)) (2008).

Absent data or feedback from the courts demonstrating that the Commission's rationale for aggregating the factors in subsection (b)(15) was flawed, or results in sentences that generally do not reflect the seriousness of the offense, the Commission should not take any action in response to these directives.

§ 209(b)(12) Whether the term "victim"as used in USSG § 2B1.1, should include individuals whose privacy was violated as a result of the offense in addition to individuals who suffered monetary harm as a result of the offense.

Directive 12 of Pub. L. 110-326 asks the Commission to consider whether the definition of "victim" in USSG § 2B1.1 should be expanded to include anyone whose privacy was violated as a result of the offense, in addition to individuals who suffered monetary harm. We oppose such an expansion on several grounds.

First, this issue is most likely to arise in the context of offenses involving identity theft, and the directive essentially asks the Commission to consider the extent to which the number of victims is an appropriate measure of the seriousness of the offense. The Commission has already studied this question,[3] however, and determined that reliance on the number of victims alone "can result in either overstating or understating the harm." *See* USSC, *Identity Theft Final Report*, at 26 (Dec. 15, 1999). The number of victims may overstate the harm in simple identity theft crimes where a means of identification is fraudulently used but not bred; it may understate the harm in a case where a means of identification is used to obtain other means of identification without the victim's knowledge. *Id*. The latter circumstance is more likely to cause significant emotional distress to the victim, and for that reason the Commission created a specific offense characteristic to apply in cases involving bred means of identification. *See* USSG § 2B1.1(b)(10)(C) & comment. (backg'd).

[3] *See* Pub. L. No. 105-318, Oct. 30 1998, at § 4(b)(1).

Second, the "non-monetary" harm perhaps most frequently cited by victims of affirmative identity theft is the loss of time associated with attempts to repair one's credit. Though typically thought of as a non-pecuniary harm, lost time can in fact be monetized and, when it is, the loss amount may be added to the loss figure determined under USSG § 2B1.1(b)(1), and the victim counted as a "victim" for guideline purposes under USSG § 2B1.1(b)(2). *See United States v. Armstead*, ___ F.3d ___, 2008 WESTLAW 4570608 (9th. Cir. Oct. 15, 2008); *United States v. Abiodun*, 536 F.3d 162, 167-69 (2d Cir. 2008). Importantly, in this regard the guidelines define "victim" co-extensively with those who may obtain restitution under 18 U.S.C. § 3663, which was amended by Pub. L. No. 110-326 to permit restitution in identity theft prosecutions for "the value of the time reasonably spent by the victim in an attempt to remediate the intended or actual harm[.]"

Third, where a court perceives that the number of individuals whose personal data was stolen in a given case is extraordinary, and not otherwise accounted for in determining the base offense level, the court may upwardly depart pursuant to USSG § 2B1.1, comment. (n.19).[4] That is precisely what the district court did in *United States v. Uyaniker*, 184 Fed. Appx. 856 (11th Cir. 2006).[5] Absent data which shows that courts are routinely upwardly departing on this basis, the Commission should not broaden the definition of "victim" beyond its current parameters.

Finally, if the Commission broadens the definition of "victim" in USSG § 2B1.1, sentences for some defendants in identity theft cases will be raised. We have seen no data which indicates that sentences in these cases are not sufficient already. To the contrary, with the passage of the Identity Theft Penalty Enhancement Act in 2004, Congress provided for a two-year, minimum mandatory, consecutive sentence to be imposed where identity theft is committed in relation to a broad range of federal felony offenses. *See* 18 U.S.C. § 1028A(a)(1) and (b). As stated above, we believe that this statute provides more than adequate punishment for the crime of identity theft.[6]

---

[4] Application Note 19(A)(vi) enumerates upward departure grounds where a victim (or victims) suffered extraordinary non-pecuniary harm, and that provision appears to provide sufficient guidance in such cases. *See, e.g., United States v. Shough,* 239 Fed.Appx. 745 (3d Cir. 2007)(affirming upward departure where defendant essentially assumed victim's identity and caused substantial harm to victim's credit rating).

[5] Although the opinion in *Uyaniker* is less than clear on this point, the Eleventh Circuit affirmed a district court's four-level upward departure based on the fact that the defendant had stolen and used the identities of 78 people. A transcript of the sentencing hearing is on file with the undersigned.

[6] *See* Erik Camayd Freixas, *Interpreting after the Largest ICE Raid in US History: A Personal Account*, June 13, 2008, *referenced in* Editorial, *The Shame of Postville, Iowa*, N.Y.Times, July 13, 2008, available at http://www.nytimes.com/2008/07/13/opinion/13sun 2.html?scp=3&sq=postville&st=cse. A copy of Dr. Camayd Freixas' article is attached.

§ 209(c)(2) [M]itigating circumstances that might justify exceptions to the generally applicable sentencing ranges[.]

At the meeting on November 20th, Commissioner Howell asked whether the Defenders could articulate mitigating factors which might constitute grounds for downward departures in identity theft or computer crimes cases. We appreciate the invitation to speak to this issue, and are considering proposals to submit in this regard. We begin by offering the following proposed language to be added to Application Note 19:

(C) Downward Departure Considerations.---There may be cases in which the offense level determined under this guideline substantially overstates the seriousness of the offense. In such cases, a downward departure may be warranted. The following is a non-exhaustive list of factors that the court may consider in determining whether a downward departure is warranted:

(i) A primary objective of the offense was a non-aggravating, non-monetary objective. For example, a primary objective of the offense was to gain access to one's own work product or to assist another person in accomplishing a non-aggravating, non-monetary objective

(ii) The offense was committed through the use of readily available computer technology, software, or hardware, which persons of average computer skills are able to operate.

(iii) The defendant acted promptly after law enforcement detection or apprehension to assist in ensuring that personal information obtained was not disseminated, or that personal information disclosed was not further disseminated.

(iv) The defendant successfully participated in a restorative justice meeting involving both the defendant and the victim. For purposes of this departure ground, "restorative justice meeting" means a face-to-face meeting moderated by a trained third party mediator in which the defendant and the victim reach agreement on reasonable steps the defendant will take to repair the harm done to the victim.

Finally, we understand that the Commission will be analyzing data as part of the study prompted by Pub. L. 110-326, § 209. We hope that you will share the results of that data analysis with us.

Sincerely,

/s/ J. Martin Richey
J. Martin Richey,
Assistant Federal Public Defender

Jennifer Coffin, Staff Attorney
Sentencing Resource Counsel

On Behalf of the Federal Public and Community Defenders and the Federal Defender Sentencing Guidelines Committee

cc: Hon. Ruben Castillo, Vice Chair
Hon. William K. Sessions III, Vice Chair
Commissioner Michael E. Horowitz
Commissioner Beryl A. Howell
Commissioner Dabney Friedrich
Commissioner Ex Officio Edward F. Reilly, Jr.
Commissioner Ex Officio Jonathan Wroblewski
Judith M. Sheon, Staff Director
Ken Cohen, General Counsel
Kathleen Grille, Deputy General Counsel